Shaping Industry Interaction Through Secure Information Sharing

Part III: Putting Theory Into Practice

Paul Grant ▪ *Jim Cisneros* ▪ *Jeff Nigriny*

The Transglobal Secure Collaboration Program (TSCP) is a global consortium involving the U.S. Department of Defense, the United Kingdom Ministry of Defence (MoD), the Netherlands Ministry of Defence, and seven of the world's largest aerospace and defense (A&D) companies. These parties have come together to address one problem: how to securely share information to enable collaboration throughout the A&D global community.

This is the final installment in a three-part series, "Shaping Industry Interaction Through Secure Information Sharing." Part II, published in the previous issue, examined the collaboration efforts of the TSCP to set industry-wide specifications for secure collaboration. The series has explored the nature of the problem of securing external data transfer, the value organizations can gain by overcoming the obstacles, and how the TSCP has embraced collaborative best practices to establish and deliver collaboration solutions to the broader community. Now, TSCP's vision is being realized in the field. The Army's Future Combat System (FCS) program was an early candidate ideally suited to take advantage of the advanced security specifications the TSCP has published over the past five years. Below, we share some of the specifics of its implementation and benefits.

Overcoming the inherent barriers to A&D collaboration is the primary industry-level challenge faced by government-industry partnerships. In the past, DoD agencies working with commercial contractors relied on a government-to-company model in which the agency swore the supplier to absolute secrecy on the project. Secrecy is still a big part of defense work, but two key differences exist today:

1. The commercial firms on which agencies have relied for decades provide services for worldwide governments and have operations in nearly every country—industries are no longer geopolitically aligned.

2. Today, large defense acquisitions typically involve named prime contractors and some number of named subprime contractors. After the contract is awarded, a supply chain is created and there is a need to share information. However, even the strongest contracts cannot guarantee that information will be seen by only the intended recipients, or that the intended recipients truly have a need to know.

In both cases, it is essential to know who is on the other end of a document exchange, communication, or signed form. This identity management requirement is central to secured collaboration. U.S. policy documents NIST Special Publication 800-63 and HSPD-12/FIPS 201 express the importance of such secure collaboration.

Once assurance in another party's identity can be ascertained, all of the classical security problems still exist, but these problems can be solved in previously unknown ways. Data no longer needs to be tied to the originating application or server. Data owners no longer have to lose control over how their data are being used in a remote network or for how long. We have long allowed global supply chains to be artificially constrained by information technology systems that do not scale. How, then, do we trust data to move from system to system and country to country, across the Internet—across what is sometimes described as a hostile network?

Allowing Trust Between Parties

The TSCP has published and is publishing systems specifications that allow end points to be trusted. End points are the sending and receiving systems for sensitive data that must be secured. If you consider the importance of identifying individuals and judging whether they are trustworthy before sharing sensitive information, this same logic dictates that the actual systems handling the data exchange and presentation must also be judged as trustworthy. However, judging a system as trustworthy is different from judging individuals. People are judged as trustworthy based on previous actions, which is an imperfect system, of course, because past behavior is not a perfect predictor of future actions. In computer systems,

---

Grant *is the deputy information sharing executive for the Department of Defense.* **Cisneros** *is the deputy CIO for the Future Combat Systems at Boeing.* **Nigriny** *is president of CertiPath and chief security officer for Exostar.*

The current and future specifications of the TSCP are designed to achieve a predictable and repeatable set of behaviors for the systems originating, sending, and receiving sensitive data.

though, understanding how a system will act in a given set of circumstances can be near perfect.

The current and future specifications of the TSCP are designed to achieve a predictable and repeatable set of behaviors for the systems originating, sending, and receiving sensitive data. If all systems in the trust fabric do not adhere to the same specification, then two critical qualities are lost. First, trust is not possible because behavior is not predictable, and second but equally important, scalability is lost. DoD has stated that there are 300,000 supplier organizations in which it wished to have a greater degree of identity assurance. This doesn't even begin to describe the scope of the individuals represented by that many organizations. Without a free and public specification that all can implement, DoD's requirements would be impossible to meet, as would the global demand for

secure information sharing. The goal of the TSCP is to establish such secure information sharing.

The Art of Information Sharing

Present thinking about information security in the supply chain can be described as a best-case scenario, ready to quickly excuse the obstacles of legacy systems and corporate cultures resistant to change. Fans of Harvard Business School case studies will be familiar with what it takes to tear down those barriers for large, complex organizations: a clear, compelling case for competitive advantage.

The security models and techniques that follow are radical enough to represent disruptive technologies in larger organizations—the key ingredient in creating an opportunity to gain competitive advantage. While it is perhaps unusual to think of IT security as an area in which competitive advantage could be gained, that is just part of what makes

this new model so disruptive. For the risk averse, there is also good news. The new models and techniques have already been widely accepted as the only realistic way to solve the problems of identity, authentication, and access control among government and industry security organizations alike.

TSCP and Future Combat Systems

The Boeing Company's FCS Program has a very large supply chain that is representative of large A&D programs today. Within Boeing, there are efforts under way intended to support programs like FCS and to leverage the work being done to promote the use of secure identification and authentication technologies. These efforts will provide Boeing programs with improved capabilities to protect data and information being exchanged electronically while working with this large supply chain of partners. There are, in fact, three areas in which Boeing is working to pilot and validate approaches within FCS, in cooperation with the TSCP and with the goal of moving towards a production capability with the Army's support.

The first area is in the use of secure medium-assurance hardware certificates. Boeing has recently conducted a successful pilot with the Army Knowledge Online group. AKO is the host for the collaborative tools used by FCS to support its need to hold virtual meetings. FCS team members originally used less-secure user names and passwords to obtain AKO access. Working with AKO leadership and the AKO technical support team, Boeing was able to apply its secure medium-assurance hardware certificates to log into the AKO environment. The success of the pilot was communicated to the DoD Identity Protection and Management Senior Coordinating Group, where the results were well received. The IPMSCG consists of general officer and senior civilian representatives from each of the military services, joint staff, the Office of the Secretary of Defense, and DoD organizations. The IPMSCG focuses on ways to use identity management tools while protecting an individual's privacy. Follow-on steps to prepare for production implementation are being planned.

A second area being addressed within FCS is improving how Boeing, as the FCS lead systems integrator, provisions accounts and authorizes access to the FCS Advanced Collaborative Environment, which houses a majority of the information being produced and used on FCS today. The FCS ACE supports the program by providing a collaborative environment through which FCS team members can deposit and share information and take advantage of capabilities like automated workflows to improve the approval and configuration management of the information generated in support of FCS. Boeing, to date, has had to provision accounts for each of its suppliers assigned to the FCS program for access to the FCS ACE. When suppliers want to gain access to the FCS ACE, they access the Web site, respond to an authentication challenge, and are

granted or denied access accordingly. While this model works, using the same authentication approach used by the AKO pilot offers improved access control and administration features. In the current model, Boeing needs to be notified when an FCS team member has left the program, so that the access privileges can be removed. Additionally, should people forget their password or require an update to any personal attributes, Boeing must expend resources to service the request. If something changes in a person's status so that he is no longer assigned to the FCS program, Boeing is dependent on the partner organization to remember to inform Boeing that the person's access needs to be revoked. Using the medium-assurance hardware approach from a cross-certified provider, each partner would then be responsible for verifying when employees exit the program or leave the company for whatever reason, and Boeing would not have to expend resources to track this information.

Identity federation provides a solution to all these problems and, when combined with a single strong credential leveraged with all partners, eliminates the inherent risk found in today's password-based approach for authentication.

The third area that FCS is seeking to address is in the use of medium-assurance hardware/software (or class 3) certificates in the secure e-mail area. FCS currently uses business-to-business, or B2B, encryption to exchange encrypted and digitally signed e-mail. This provides encrypted e-mail on a user-to-user basis across company/partner boundaries utilizing basic-assurance (class 2) certificates. The expected benefits of moving to class 3 certificates would be to demonstrate Boeing's alignment with DoD's plan for adopting advanced public key infrastructure and further outline the value proposition for using class 3 certificates. It will also demonstrate the reduced time/cost for configuring infrastructure for bilateral trust and configuring systems to establish trust in the validity of CertiPath, the A&D industry's PKI bridge. This pilot will additionally assist in identifying any interoperability issues between class 2 and 3 infrastructures, provide an understanding of what and which PKI and e-mail products need to be modified or improved, and identify where and what infrastructures are not in a state of readiness among Boeing's tier 1 suppliers—otherwise known as FCS One Team Partners.

The fact that a number of the TSCP participant companies are also FCS One Team Partners make this a win-win situation as FCS presses forward in testing and verifying these capabilities.

A Shared Commitment to Collaboration Excellence

The FCS is one example that demonstrates the value of secure information-sharing strategies in enhancing the

The idea that we can control data at a granular enough level to define the who, when, and how of receipt has the potential to give us confidence that our data won't be accessed inappropriately or in a manner inconsistent with our wishes as the data owner—the aim of information security in the first place.

department's efficiency and effectiveness. In the near future, DoD hopes to recognize some of the potential benefits for other major acquisition programs in becoming early adopters of the TSCP output, including JSF, DDx (a U.S. Navy destroyer ship in design), and Alliance Ground Surveillance.

DoD's intention is to provide better guidance on compliant use of data, which will aid the implementation of DoD policy in areas such as the unique identification of tangible assets and the achievement of net-centricity, with inherent data-segregation management and federated, collaborative identity and access management.

Looking ahead, major initiatives for DoD and the TSCP are intellectual property protection and export control inside a product life cycle management environment, and then the same intellectual property protection and export control in real-time collaboration (for example, online whiteboarding—a capability that enables globally located conference attendees to annotate and draw collaboratively on shared images or slides appearing on the screen).

A key enabler of these next two initiatives is a technology and policy concept called digital rights management. DRM provides the mechanism through which trust can be extended from the data owner to a single data recipient, even at a remote organization. The idea that we can control data at a granular enough level to define the who, when, and how of receipt has the potential to give us confidence that our data won't be accessed inappropriately or in a manner inconsistent with our wishes as the data owner—the aim of information security in the first place.

The authors welcome comments and questions and can be contacted at paul.grant@osd.mil, james.m.cisneros@boeing.com, and jeff.nigriny@certipath.com.